SECURE BOOTSTRAPPING ARCHITECTURE METHOD BASED ON PASSWORD-BASED DIGEST AUTHENTICATION

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation of U.S. patent application Ser. No. 12/918,856, filed on Feb. 28, 2011, which is a US Utility Application of PCT Application Serial Number PCT/EP2008/001479, filed on Feb. 25, 2008, both of which are incorporated by reference herewith in their entirety.

FIELD OF THE INVENTION

[0002] The present invention relates to a method and apparatus for performing authentication between a client and a server, and more specifically to a secure bootstrapping mechanism based on password-based Hypertext Transfer Protocol (HTTP) digest authentication.

BACKGROUND OF THE INVENTION

[0003] Security of mobile terminals, such as portable communication devices (e.g., cellular telephones or user equipments (UEs)), portable digital assistants, laptop computers, or any suitable device that is capable of communicating with a wireless network, is increasingly important to mobile terminal users. Security algorithms may be employed to achieve security between a mobile terminal and another network entity. These security algorithms often rely upon a secret that is shared between the mobile terminal and the other network entity which permits the mobile terminal to be authenticated. Typically, this shared secret is embodied in a form of a key.

[0004] A bootstrapping server function (BSF) is an intermediary element in cellular networks which provides application independent functions for mutual authentication of mobile terminals and servers are known to each other and for bootstrapping the exchange of secret session keys afterwards. This allows use of additional services which need authentication and secure communication. In this case, the term "bootstrapping" is related to building a security relation with a previously unknown device first and to allow installing security elements (e.g. keys) in the device and the BSF afterwards. The setup and function to deploy a generic security relation is sometimes called generic bootstrapping architecture (GBA) or generic authentication architecture (GAA).

[0005] The GBA as specified in 3rd generation partnership protocol (3GPP) specification TS 33.220 is currently based on the fact that a user is in possession of a user identity module (e.g. a universal integrated circuit card (UICC) or subscriber identity module (SIM)) on which an authentication and key agreement (AKA) mechanism can be run. GBA has defined a generic mechanism that allows, based on a route secret stored in the user identity module, to generate and use derived secrets between the UE and different applications in a network. The GBA mechanism allows for different applications in the networks and terminals to avoid a large diversity of authentication mechanisms and allows addressing security issues once in a consistent way.

[0006] Authentication to HTTP based application servers owned by fixed network operators as well as the network itself is primarily password-based. Therefore, network operators which own only fixed access may not want to introduce user identity modules for the customers only for the purpose of GBA. Developing a password-based GBA would help these operators. The GBA mechanism is useful, as it can restrict the number of stored passwords in the network and to be managed by the user.

[0007] An example of client authentication for which secure communication is highly desirable is HTTP digest access authentication which verifies that both client and server know a shared secret (e.g. HTTP password). After verification, secure communications are commenced between the client and the server. The HTTP digest access authentication scheme is based on a simple challenge-response paradigm. The scheme involves a challenge being issued to the client using a nonce value. In security engineering, such a "nonce" stands for "number used once" and is often a random or pseudo-random number issued in an authentication protocol to ensure that old communications cannot be reused in replay attacks. In the HTTP digest access authentication, nonces are used to calculate a hashed digest of a password. Hashing may be based on an application of e.g. MD-5 cryptographic hashing. The nonces are different each time an authentication challenge response code is presented, and each client request has a unique sequence number, thus making the replay attack virtually impossible. A valid HTTP response to the challenge verifies knowledge of the shared secret.

[0008] According to a known authentication mechanism for using GBA based on HTTP digest (also known as GBA_H), changes to standard browsers including transaction layer security (TLS) are required, so that the UE and the BSF can access the TLS master secret for use in GBA. Furthermore, the GBA_H mechanism is vulnerable to a Main-In-The-Middle (MITM) attack where the attacker runs a TLS session with the BSF and interacts with the UE via HTTP outside of the TLS tunnel. The MITM needs to trick the UE into communication with the MITM using HTTP digest outside TLS. In order to achieve this, the MITM could be a corrupted server or an additional installed server, and the user could be tricked (e.g. by e-mail and/or social engineering techniques) to contact the MITM server requiring the user to run HTTP digest. Furthermore, users are not always aware when a secure connection is required or active in their browser.

[0009] Additionally, a 2G GBA solution is described in Annex I of TS 33.220 and uses TLS between the UE and the BSF. This solution ensures that the entropy of the bootstrapped key is greater than the entropy which can be reached by using one 2G authentication vector. At the same time, this solution is not vulnerable to the MITM attack. The bootstrapped key is derived from both the authentication result and some information which is transmitted inside the TLS tunnel. However, 2G GBA uses HTTP digest AKA for authentication and thus requires the root secret to be securely stored in a user identity module.

[0010] Therefore, a secure bootstrapping mechanism based on password-based HTTP digest authentication would be desirable, which alleviates at least one of the drawbacks of susceptibility to vulnerabilities of known HTTP digest based solutions, lack of key freshness for the bootstrapped key, lack of forward secrecy due to password disclosure and its effect on a bootstrapped key generated before the pass-